(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

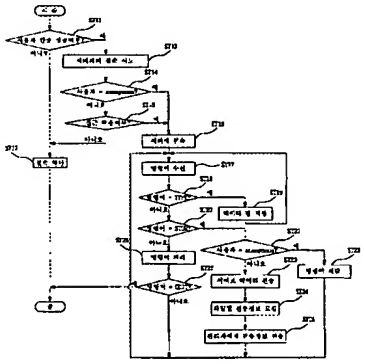
(11)Publication number: 1020020001190 A
(43)Date of publication of application: 09.01.2002

(21)Application number: 1020000035533
(22)Date of filing: 27.06.2000
(51)Int. Cl H04L 12 /22

(71)Applicant: LG ELECTRONICS INC.
(72)Inventor: LEE, SANG U

(54) SECURITY SYSTEM HAVING REINFORCED PROTECTION FUNCTION FOR INTERNAL RESOURCES IN NETWORKS AND OPERATING METHOD THEREOF

(57) Abstract:



PURPOSE: A security system having a reinforced protection function for internal resources in networks and an operating method thereof are provided to monitor and trace an external leakage of internal resources as an FTP(File Transfer Protocol) proxy monitors internal clients FTP service usage status and executes real-time monitoring for the copy storage and transmission information of the data being transmitted to the external. CONSTITUTION: An FTP proxy, receiving an FTP service access request for an external network from an internal network user, determines whether the user has the authority to access the external network(ST11). If the access authority for the external network is authenticated for the user, the user attempts access to an FTP server(ST13). In case that the internal network user attempts access to the FTP server with an anonymous account, access is granted to him without any special access control operation. However, in the case that the user attempts access with a specific account, the FTP proxy confirms whether it is an access request from a client granted to the specific account and executes access control(ST15).

Legal Status
Date of request for an examination (20000627)
Notification date of refusal decision ( )
Final disposal of an application (registration)
Date of final disposal of an application (20020925)
Patent registration number (1003583870000)
Date of registration (20021012)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )

Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04L 12/22

(11) 공개번호 특2002 -0001190
(43) 공개일자 2002년01월09일

(21) 출원번호 10 -2000 -0035533
(22) 출원일자 2000년06월27일

(71) 출원인 엘지정보통신주식회사
서평원
서울 강남구 역삼1동 679

(72) 발명자 이상우
인천광역시남동구간석1동금호아파트2동307호

(74) 대리인 홍성철

심사청구 : 있음

(54) 네트워크망에서 내부자원의 보호기능이 강화된 보안장치및 그 운용방법

요약

본 발명은 방화벽의 후단에 구비된 FTP 프락시가 내부 클라이언트들의 FTP 서비스 이용현황을 감시하여 실시간 모니터링을 수행함으로써 내부자원의 외부유출을 방지할 수 있는 네트워크망에서 내부자원의 보호기능이 강화된 보안장치 및 그 운용방법을 제공하기 위한 것으로, 방화벽과; 내부망으로부터 외부망으로의 접근요구에 대한 인증여부를 판단하고 인증된 사용자가 외부망으로 전송하는 데이터의 복사본 및 로그정보를 저장하는 FTP 프락시로 구성되는 장치와,

내부사용자의 외부서버에 대한 접근권한의 인증을 수행하는 단계와; 출력되는 데이터형을 저장하는 단계와; 전송권한이 인증된 사용자의 데이터를 서버로 전송하고 전송되는 파일의 복사본 및 로그정보를 저장하는 단계와; 각 명령어에 따른 동작을 수행하고 접속종료 명령어가 있게 되면 서버와의 접속을 종료하는 단계로 구성되는 방법을 수행하여, 내부사용자의 FTP 서비스를 이용한 자원유출을 감시/추적하고 실시간 모니터링할 수 있는 것이다.

대표도
도 3

명세서

도면의 간단한 설명

도1은 종래기술에 의한 네트워크망의 보안장치의 블록구성도이고,

도2는 본 발명의 일실시예에 의한 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 블록구성도이고,

도3은 본 발명에 의한 장치에 적용되는 운용방법의 흐름도이고,

도4는 도3에서 파일 및 로그정보 저장동작의 상세흐름도이며,

도5는 도4에서 로그정보의 구성예시도이다.

* 도면의 주요 부분에 대한 부호의 설명 *

11 : 방화벽 12 : FTP 프락시 13 : 클라이언트

14 : FTP 서버 15 : 프락시 모니터

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크망의 보안기능에 관한 것으로, 특히 인터넷(Internet) 등의 공중 네트워크망에 접속되는 내부 네트워크에서 FTP 프락시(File Transfer Protocol Proxy)가 내부 클라이언트들의 FTP 서비스 이용현황을 감시하여 내부에서 외부로 전송되는 데이터의 복사본 저장 및 전송정보의 실시간 모니터링을 수행함으로써, 내부자원의 외부유출을 감시하고 추적할 수 있도록 한 네트워크망에서 내부자원의 보호기능이 강화된 보안장치 및 그 운용방법에 관한 것이다.

일반적으로 인터넷과 같은 공중 네트워크망에 접속되는 내부 네트워크망을 구성하는 경우에 있어서, 내부 네트워크에서는 자유롭게 공유되는 자원일지라도 외부망으로의 유출을 방지할 필요가 있다. 상기와 같이 특정의 자원에 대한 보안기능은 일반적으로 방화벽을 통해 구현되는데, 특히 내부적으로 중요한 자원의 외부유출을 방지할 필요가 있는 경우 방화벽에 대하여 높은 신뢰성을 요구하게 된다.

이하, 네트워크망의 보안기능에 대한 종래기술을 설명한다.

먼저, 도1은 종래기술에 의한 네트워크망의 보안장치의 블록구성도이다.

상기 도1에 도시된 바와 같이 네트워크망은, 외부망으로부터 내부망으로의 접근요구에 대한 차단기능을 선별적으로 수행하는 방화벽(1)과; 인터넷을 통해 상기 방화벽(1)의 인증을 받아 FTP 서버(3)로 접속하는 복수개의 클라이언트(2)와; 상기 복수개의 클라이언트(2)의 접속요구를 수용하여 데이터 교환을 수행하는 FTP 서버(3)로 구성된다.

상기 구성에 따른 장치의 동작을 설명하면 다음과 같다.

일반적으로 외부망에 대하여 FTP 서비스를 제공하는 내부망의 방화벽(1)에는 FTP 프락시가 구비되어 있으며, 상기 FTP 프락시가 내부망에 대한 접속요구를 발하는 외부망의 클라이언트(2)에 대한 인증여부를 결정하게 된다. 즉, 내부 네트워크의 특정 데이터에 대한 사용자의 접근요구를 접수하여 허가된 사용자인지 아닌지를 판단함으로써, 내부 네트워크로의 접속허용 여부를 결정하여 내부 데이터를 보호하는 기능을 수행하게 된다. 따라서 방화벽의 FTP 프락시는 서비스를 요청하는 주체와 서비스를 요청받는 객체사이의 접근제어와 사용자를 확인하기 위한 사용자 인증방법 등을 주로 이용하여 보안기술을 구현하게 되는 것이다.

어러한 방화벽(1)에는 응용프로그램 게이트웨이(Gateway)라 하여 방화벽상에 다종의 프락시들이 존재하며, 패킷 필터링(Packet Filtering) 등의 다른 보안기능과 더불어 실행된다. 사용자 인증방법의 경우 인증서버에 의해 관리되는 일반 평문형식(Text Type)의 패스워드나 일회용 패스워드를 사용하며, 접근제어의 경우 주체와 객체의 각종 정보를 가지고 접근허용 및 차단여부를 결정한다. 이때 접근권한의 인증과 관련된 주체는 클라이언트(2)이고 객체는 내부망의 FTP 서버(3)가 된다.

그래서 외부망의 사용자가 FTP 서비스를 제공받고자 하는 경우에는 방화벽(1)상에서 실행중인 FTP 프락시에 접속하여 사용자 인증을 마친 후 FTP 서버(3)로 접속하게 된다. 다만 방화벽(1)의 기능 중 NAT(Network Address Translator)를 이용할 경우 내부사용자에 한하여 FTP 프락시를 거치지 않고 바로 외부망의 FTP 서버에 접속할 수 있다.

특히, 전형적인 FTP 프락시는 논리적으로는 하나의 접속노드를 가지지만, 물리적으로는 FTP 서버(3)와 FTP 프락시간 및 FTP 프락시와 클라이언트(2)간에 구성되는 두 개의 접속노드를 갖게 된다. 이때 FTP 프락시는 서비스를 요구한 사용자에 대한 사용자 인증을 위하여 인증서버와 메시지 교환을 수행하게 되는데, 상기 생성된 접속노드가 주체(2)와 FTP 프락시 사이의 물리적 접속노드이다.

만약, 사용자 인증에 실패하게 되면 FTP프락시에 의하여 물리적 접속노드의 접속차단이 이루어지게 될 것이다. 그리고 사용자 인증에 성공하여 물리적 접속노드가 구성되면, 사용자는 실제 접속하고자 하는 FTP 서버(3)에 대한 접속을 요청하여 FTP 프락시의 접근제어 규칙을 통과함으로써 FTP 프락시와 객체(3)간의 물리적 접속이 이루어지게 된다. 이때 상기 접근제어 규칙을 통과하지 못하게 되면 클라이언트(2)와 FTP 프락시 사이의 물리적 접속이 차단된다.

그리고 이러한 모든 접속과정 및 사용자의 행위는 FTP 프락시에 의하여 로그정보로써 기록된다. FTP 프락시가 기록하는 로그정보는 사용자 ID, 출발지 및 목적지 IP 주소, 날짜, 시간, 접속차단이유 등이며, 상기 로그정보는 시스템에의 접속통계 및 데이터 흐름의 추적자료로써 활용될 수 있게 된다.

상기 설명한 종래기술에 의한 보안기능의 경우에 방화벽상의 FTP 프락시는 외부 사용자의 내부망에 대한 접속요구시 접속허용 여부를 결정하여 내부자원을 보호하는 기능이 주목적이다. 따라서 내부 사용자에 의하여 중요한 자원이 외부로 유출될 가능성에 대하여는 보안기능이 상대적으로 취약한 문제점이 있었다.

즉, 방화벽을 기준으로 내부 사용자는 대부분 허가된 사용자이며 외부 사용자는 허가되지 않은 사용자라는 전제조건과 내부 자원을 감시하기 위한 기능의 구현시 방화벽에 큰 부하가 걸리는 점을 고려하여 FTP 프락시의 보안기능은 내부 사용자보다는 외부 사용자의 접근 통제기능을 중심으로 작용하였기 때문에, 내부 사용자가 FTP 서비스를 이용하여 내부자원을 외부로 유출시키는 것에 대한 특별한 보호수단을 갖지 못한 문제점이 있었던 것이다.

발명이 이루고자 하는 기술적 과제

이에 본 발명은 상기와 같은 종래의 제반 문제점을 해소하기 위해 제안된 것으로, 본 발명의 목적은 공중 네트워크망에 접속되는 내부 네트워크에서 FTP 프락시가 내부 클라이언트들의 FTP 서비스 이용현황을 감시하여 내부에서 외부로 전송되는 데이터의 복사본 저장 및 전송정보의 실시간 모니터링을 수행함으로써, 내부자원의 외부유출을 감시하고 추적할 수 있도록 한 네트워크망에서 내부자원의 보호기능이 강화된 보안장치 및 그 운용방법을 제공하는 데 있다.

상기와 같은 목적을 달성하기 위하여 본 발명에 의한 네트워크망에서 내부자원의 보호기능이 강화된 보안장치는, 외부망으로부터 내부망으로의 접근요구에 대한 차단기능을 선별적으로 수행하는 방화벽과; 내부망으로부터 외부망으로의 접근요구에 대한 인증여부를 판단하고, 인증된 사용자가 외부망으로 전송하는 데이터의 복사본 및 상기 데이터 전송에 관련된 로그정보를 저장하는 FTP 프락시와; 상기 FTP 프락시의 인증을 받아 외부망의 FTP 서버와 데이터를 교환하는 복수개의 클라이언트와; 인터넷상에서 내부망의 클라이언트의 접속요구를 수용하여 각종 데이터의 교환을 수행하는 복수개의 FTP 서버와; 상기 FTP 프락시의 로그정보를 수신하여 시스템 관리자가 인지할 수 있도록 출력하는 프락시 모니터와; 상기 FTP 프락시의 전송데이터 복사본을 데이터형별로 구분하여 저장하는 파일시스템과; 상기 FTP 프락시의 전송데이터에 관한 로그정보를 저장하는 데이터베이스로 이루어짐을 그 기술적 구성상의 특징으로 한다.

상기와 같은 목적을 달성하기 위하여 본 발명에 의한 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 운용방법은, 내부사용자의 외부 서버에 대한 접근권한의 인증을 수행하고, 상기에서 접근권한이 인증된 사용자가 외부 서버에 접속하는 제1 단계와; 상기 제1 단계 수행 후 사용자의 명령어를 수신하여 상기 명령어가 데이터형 지정을 요구하는 것이면 지정된 데이터형을 저장하는 제2 단계와; 상기 제2 단계에서 수신한 명령어가 데이터 송신을 요구하는 것이면 데이터 전송권한이 인증된 사용자의 데이터를 서버로 전송하고 상기 전송되는 파일의 복사본 및 로그정보를 저장하고 시스템 관리자에게 상기 로그정보를 전송하는 제3 단계와; 상기 제2 단계에서 수신한 명령어가 데이터형 지정요구 또는 데이터 송신명령이 아닐 경우에는 해당 명령어에 따른 동작을 수행하고, 접속종료 명령어가 있게 되면 서버와의 접속을 종료하는 제4 단계를 수행함을 그 기술적 구성상의 특징으로 한다.

발명의 구성 및 작용

이하, 상기와 같은 네트워크망에서 내부자원의 보호기능이 강화된 보안장치 및 그 운용방법의 기술적 사상에 따른 실시예에 의거 본 발명의 구성 및 동작을 상세히 설명한다.

먼저, 도2는 본 발명의 일실시예에 의한 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 블록구성도이고, 도3은 본 발명에 의한 장치에 적용되는 운용방법의 흐름도이고, 도4는 도3에서 파일 및 로그정보 저장동작의 상세흐름도이며, 도5는 도4에서 로그정보의 구성예시도이다.

상기 도2에 도시된 바와 같이 본 발명에 의한 장치의 적절한 일실시예는, 외부망으로부터 내부망으로의 접근요구에 대한 차단기능을 선별적으로 수행하는 방화벽(11)과; 내부망으로부터 외부망으로의 접근요구에 대한 인증여부를 판단하고, 인증된 사용자가 외부망으로 전송하는 데이터의 복사본 및 상기 데이터 전송에 관련된 로그정보를 저장하는 FTP 프락시(12)와; 상기 FTP 프락시(12)의 인증을 받아 외부망의 FTP 서버(14)와 데이터를 교환하는 복수개의 클라이언트(13)와; 인터넷상에서 내부망의 클라이언트(13)의 접속요구를 수용하여 각종 데이터의 교환을 수행하는 복수개의 FTP 서버(14)와; 상기 FTP 프락시(12)의 로그정보를 수신하여 시스템 관리자가 인지할 수 있도록 출력하는 프락시 모니터(15)와; 상기 FTP 프락시(12)의 전송데이터 복사본을 데이터형별로 구분하여 저장하는 파일시스템(16)과; 상기 FTP 프락시(12)의 전송데이터에 관한 로그정보를 저장하는 데이터베이스(17)로 구성된다.

상기 도3에서 본 발명에 의한 방법의 적절한 실시예는, 내부사용자의 외부 서버에 대한 접근권한의 인증을 수행하고, 상기에서 접근권한이 인증된 사용자가 외부 서버에 접속하는 제1 단계(ST11~ST16)와; 상기 제1 단계(ST11~ST16) 수행 후 사용자의 명령어를 수신하여 상기 명령어가 데이터형 지정을 요구하는 것이면 지정된 데이터형을 저장하는 제2 단계(ST17~ST19)와; 상기 제2 단계(ST17~ST19)에서 수신한 명령어가 데이터 송신을 요구하는 것이면 데이터 전송권한이 인증된 사용자가 전송하려는 데이터를 서버로 전송하고 상기 전송되는 파일의 복사본 및 로그정보를 저장하며 시스템 관리자에게 상기 로그정보를 전송하는 제3 단계(ST20~ST25)와; 상기 제2 단계(ST17~ST19)에서 수신한 명령어가 데이터형 지정요구 또는 데이터 송신명령이 아닐 경우에는 해당 명령어에 따른 동작을 수행하고, 접속종료 명령어가 있게 되면 서버와의 접속을 종료하는 제4 단계(ST26~ST27)로 구성된다.

그리고 상기 제3 단계(ST20~ST25)에서 외부로 전송되는 파일의 복사본 및 전송정보의 저장은, 내부망에서 외부망으로 전송되는 파일을 수신하여 상기 파일의 데이터형에 따라 복사본을 파일시스템(16)에 저장하고 외부망으로 파일을 전송하는 전송동작을 반복적으로 수행하는 단계(ST31~ST34)와; 상기 단계(ST31~ST34)에서 외부망으로의 데이터 전송이 완료되면, 상기 전송과정에 대한 정보를 로그정보로써 데이터베이스에 저장하고 상기 로그정보를 시스템의 관리자가 인지할 수 있도록 출력하는 단계(ST35~ST36)로 구성된다.

이와 같이 구성되는 장치 및 방법의 동작을 설명하면 다음과 같다.

우선 본 발명에 의한 장치는 방화벽을 갖춘 네트워크망에 구현될 수 있는 것으로, 외부망에서 내부망으로의 접근제어를 중심으로 동작하는 종래기술과는 달리, 내부망에서 외부망으로의 접근제어와 데이터 전송의 감시/추적 기능을 더 수행할 수 있게 된다.

즉, 내부망의 각 클라이언트(13)가 방화벽(11)으로 접근하는 전송로상에 FTP 프락시(12)를 구비함으로써, 내부망의 클라이언트(13)가 외부망의 FTP 서버(14)에 접속하고자 하는 경우에는 반드시 FTP 프락시(12)의 인증 및 감시를 받도록 하고 내부망에서 외부망으로의 접근제어를 수행할 수 있게 된다. 이러한 접근제어를 위하여 FTP 프락시(12)는 내부망에 구비된 각 호스트(13)의 FTP 서버(14)에 대한 접근요구를 수신하여 해당 호스트가 정당한 권한을 갖는 것인지를 확인하게 된다.

상기에서 정당한 접근권한이 인증된 호스트는 외부망의 FTP 서버(14)에 접속하여 FTP 서비스상에서 클라이언트(13)로써 동작하게 된다. 그래서 내부망의 클라이언트(13)와 외부망의 FTP 서버(14)의 접속이 이루어진 상태에서 데이터 전송이 이루어지면, FTP 프락시(12)는 전송되는 데이터의 복사본과 전송과정의 각종정보를 저장하는 한편 프락시 모니터(15)로 전송하게 된다.

그리고 FTP 서버(14)와 클라이언트(13)는 제어접속(Control Connection)을 통해 FTP 명령어(Command)와 응답(Reply)을 교환한다. 이때 FTP 명령어는 3 또는 4바이트의 문자열로 구성되고, 명령어에 따라서는 임의의 가변인자를 더 포함하기도 한다. 상기와 같은 명령어에 대한 응답은 3자리의 숫자열로 구성되고, 상기 숫자열에 이어 부가적인 메시지를 전송하게 된다. 또한, FTP 서버(14)와 클라이언트(13)간의 데이터 교환은 데이터 접속을 통하여 이루어지는데, 교환되는 데이터는 파일과 디렉토리 목록이 된다.

상기 설명한 장치의 동작은 그 운용방법을 설명함으로써 보다 구체화될 수 있다.

본 발명에 의한 방법에서 내부보안을 수행하는 FTP 프락시(12)는 FTP 서비스 이용자를 확인하기 위한 인증기능과 각 사용자들이 허가된 호스트로부터 접속을 시도했는지에 대한 접근제어 기능과, 외부로 전송하는 파일에 대한 로깅(logging)기능 및 상기 로깅으로 생성된 로그정보를 데이터베이스에 저장하는 감시기록 기능 및 시스템 관리자에게 상기 로그정보를 실시간으로 통지하는 모니터링 기능을 수행하게 된다.

즉, 내부망의 클라이언트(13)로부터 외부망에 대한 FTP 서비스 접속요구를 수신하는 FTP 프락시(12)는 시스템내에 등록된 계정 및 패스워드 검사를 통하여 외부망에 대한 해당 사용자의 접근권한 여부를 결정한다(ST11). FTP 프락시(12)는 인증이 거부된 사용자의 물리적 접속노드에 대해서는 접속차단을 수행하게 된다(ST12). 그래서 외부망에 대한 접근권한이 인증된 사용자에 대해 FTP 프락시(12)가 물리적 접속을 허용하게 되면, 내부망의 클라이언트(13)는 해당 FTP 서버(14)에 접속시도하게 된다(ST13).

상기에서 내부망의 사용자가 anonymous 계정으로 FTP 서버(14)에 접속시도하는 경우에는 별다른 접근제어 동작없이 접속이 허용되지만(ST14), 특정의 계정으로 외부망의 FTP 서버(14)에 접속시도하는 경우에는 상기 특정의 계정에 허가된 클라이언트(13)로부터의 접근요구인지를 확인하여 접근제어를 수행하게 된다(ST15). 그러므로 정당한 계정을 갖는 사용자로써 인증된 경우에도 해당 계정에 대해 허가된 클라이언트(13) 이외의 시스템을 통하여 접속시도하게 되면, FTP 프락시(12)는 접근제어를 수행하여 클라이언트(13)와 FTP 서버(14)간의 물리적 접속을 차단하게 되

눈 것이다(ST12).

그리고 외부망의 FTP 서버(14)에 대한 내부 사용자의 접속요구 계정이 anonymous 로써 불특정 사용자인 경우와 특정계정에 대하여 접근이 허용된 경우에는 해당 사용자가 사용중인 클라이언트(13)와 외부망의 FTP 서버(14)간의 물리적 접속이 이루어진다(ST16). 이처럼 FTP 서버(14)에 접속된 클라이언트(13)는 상기 FTP 서버(14)에 대해 일정한 명령처리를 요구할 수 있게 된다.

상기에서 사용자 인증은 FTP 프락시(12)가 사용자의 계정에 대한 패스워드 검사를 수행하여 이루어진다. 그리고 접근제어는 사용자 계정의 등록시 상기 계정으로 외부망에 접속할 수 있는 호스트를 특정하여 등록시킨 후 어떤 호스트로부터 접근요구 발생시 해당 호스트와 사용자의 계정을 비교하여 허가된 접근요구인지를 판단함으로써 이루어진다. 이때 anonymous 계정으로 접속을 시도하는 경우에는 FTP 프락시(12)에 의한 패스워드 검사와 접근제어 동작은 수행되지 않지만, anonymous 계정으로 FTP 서버에 접속하는 사용자에 대해서는 해당 FTP 서버(14)로의 파일전송을 위한 put 또는 mput 등의 파일전송 명령을 제외한 명령어 사용만이 허용된다.

따라서 파일을 외부로 전송하기 위해서는 내부망의 사용자는 등록된 계정을 확보하여야 한다. 사용자에 대한 계정부여는 시스템 관리자에 의해 수행될 수 있으며, 계정부여시 사용자가 상기 계정으로 FTP 접속할 때 이용할 호스트를 지정하도록 한다. 즉, 사용자 계정으로 접속요구할 수 있는 호스트를 특정하여 허가된 호스트를 이용하는 사용자에 대해서만 외부망의 FTP 서버(14)에의 접속을 허용하는 것으로, FTP 서비스를 요청한 호스트와 등록된 호스트의 비교를 통해 하나의 계정으로 다수의 사용자가 서비스를 이용하는 것을 방지할 수 있게 된다.

상기의 동작으로 외부망의 FTP 서버(14)에 접속된 호스트는 FTP 서비스의 클라이언트(13)로써 동작하며, FTP 프락시(12)는 상기 클라이언트(13)가 FTP 서버(14)로 전송하는 명령어를 수신하여(ST17) 상기 수신된 각 명령어에 따른 로그정보의 기록을 수행하게 된다. 즉, FTP 프락시(12)는 수신되는 명령어가 데이터형 지정요구 명령인 TYPE 인 경우에는(ST18), 지정된 데이터형 정보를 메모리에 저장하게 되고(ST19), 명령어가 데이터 송신명령인 STOR 인 경우에는(ST20) 사용자 계정이 anonymous 인지 확인하게 된다(ST21).

상기에서 사용자 계정이 anonymous 이면, FTP 프락시(12)는 사용자의 데이터 송신명령을 차단하여 데이터가 외부망으로 전송되는 것을 방지하게 된다(ST22). 그리고 사용자 계정이 anonymous 가 아니면, 외부망의 FTP 서버(14)로 해당 데이터를 전송하고(ST23) 상기 전송되는 데이터를 구성하는 파일의 복사본을 FTP 프락시(12)의 파일시스템(16)에 저장하고 로그정보를 데이터베이스(17)에 기록하게 된다(ST24). 이때 데이터베이스(17)에 기록되는 로그정보와 복사본 파일의 저장경로는 시스템의 관리자에게도 전송되어 FTP 서비스 현황에 대한 실시간 감시 및 추적이 가능하도록 한다(ST25).

특히, 도5에 도시된 바와 같이 외부망으로 데이터 전송시 기록되는 로그정보는 파일전송을 수행하는 사용자의 계정, 상기 사용자가 사용중인 클라이언트(13)의 IP 주소, 해당 파일이 전송되는 FTP 서버(14)의 IP 주소, 파일 전송시의 날짜 및 시간, 클라이언트(13)에서 FTP 서버(14)에 저장되는 파일명 및 절대경로, FTP 프락시(12)상에 로깅(Logging)된 파일의 절대경로와 파일명 등으로 이루어진다. 이때 저장되는 복사본 파일의 경우 FTP 프락시(12)상에 저장되기 때문에 파일명이 중복될 가능성이 있지만, 시간상 늦게 저장되는 파일명 뒤에 일련의 숫자를 부가하는 방식으로 유일한 파일명을 구성함으로써 기 저장된 복사본 파일이 덮어쓰기(Overwrite)로 인해 유실되는 것을 방지할 수 있다.

고리고 외부망의 FTP 서버(14)에 접속된 클라이언트(13)가 데이터 송신과 관련된 명령어 이외의 명령처리를 요청하는 경우에는 FTP 프락시(12)는 별다른 동작을 수행하지 않고, 해당 명령어가 FTP 서버(14)로 전송되어 처리되도록 한다(ST26). 이러한 각 명령어에 따른 동작수행은 필요한 횟수만큼 반복적으로 수행되고, 클라이언트(13)로 접속종료 명령어인 QUIT 가 입력되면 FTP 서버(14)와 해당 클라이언트(13)간의 접속이 중단된다(ST27).

상기에서 외부망으로 전송되는 파일의 복사본 저장 및 로그정보 저장동작은 첨부한 도4에 도시된 바와 같이, FTP 서비스에 접속하는 내부망의 클라이언트(13)가 FTP 서버(14)로 전송하려는 파일을 FTP 프락시(12)가 수신하여(ST31) 상기 파일을 파일형식에 따라 구분하여 파일시스템(16)에 저장하게 된다(ST32). 일반적으로 파일형식에는 ASCII(American Standard Code for Information Interchange)형과 EBCDIC(Extended Binary Coded Decimal Interchange code)형 및 이미지(Image)형이 있다.

이처럼 데이터형을 구분저장하는 것은 각 파일의 유지관리 및 호환성 등을 고려한 것이며, 전송파일에 대한 데이터형의 구분이 불가능하거나 상기 열거된 3가지 파일형식 이외의 형식을 갖는 파일이 수신되는 경우에는 기본적으로 이미지형으로 분류하여 저장하게 된다.

상기의 동작으로 FTP 프락시(12)에 의한 수신데이터의 파일형식별 구분저장이 수행되면, 해당 데이터는 FTP 서버(14)로 전송된다(ST33). 이어서 FTP 프락시(12)는 클라이언트(13)로부터 수신되는 데이터가 더 있는지를 확인하여 수신데이터가 있으면(ST34), 상기 파일형식별 구분저장 동작 및 데이터 전송동작을 반복적으로 수행하게 된다.

그래서 모든 데이터의 전송이 완료되어 클라이언트(13)로부터 수신되는 데이터가 없게 되면, FTP 프락시(12)는 상기 데이터 전송과정상의 로그정보를 데이터베이스(17)에 저장한다(ST35). 또한, 로그정보는 프락시 모니터(15)로 전송되어 표시됨으로써, 관리자가 FTP 서비스 현황을 실시간으로 감시/추적할 수 있도록 한다.

이처럼 본 발명은 방화벽이 구비된 네트워크상에서 내부망으로부터 외부망을 향한 FTP 서비스를 감시할 FTP 프락시를 구비하여 사용자의 인증기능을 수행하고, 내부망에서 외부망으로 전송되는 데이터 및 상기 데이터의 전송과 관련된 각종 정보를 저장하며, 시스템 관리자의 FTP 서비스 현황에 대한 실시간 감시가 가능하도록 하는 것이다.

이상에서 본 발명의 바람직한 실시예를 설명하였으나, 본 발명은 다양한 변화와 변경 및 균등물을 사용할 수 있다. 본 발명은 상기 실시예를 적절히 변형하여 동일하게 응용할 수 있음이 명확하다. 따라서 상기 기재 내용은 하기 특허청구범위의 한계에 의해 정해지는 본 발명의 범위를 한정하는 것이 아니다.

발명의 효과

이상에서 살펴본 바와 같이 본 발명에 의한 네트워크망에서 내부자원의 보호기능이 강화된 보안장치 및 그 운용방법은, 방화벽이 구축된 네트워크 시스템에서 내부 사용자가 FTP 서비스를 이용하여 내부망의 중요자원을 외부로 유출시키는 것에 대한 보안관리가 취약하였던 종래기술의 문제점을 극복하고, 허가된 사용자에 대해서만 외부망에 대한 파일전송 권한을 부여함으로써 내부자원의 보안관리 기능을 향상시키는 효과가 있다.

그리고 등록된 계정을 가지고 있어 외부망에의 접근이 허가된 사용자의 경우에도 내부망에서 외부망으로 전송하는 파일에 대한 복사본 및 로그정보를 기록하여 파일이동 현황의 감시/추적이 가능하고 FTP 서비스 현황에 대한 실시간 모니터링이 가능하도록 하는 효과를 갖는다.

이처럼 실시간 모니터링을 수행함으로써 내부의 중요자원이 외부로 유출되는 것을 최대한 방지하고 상황에 따라서는 실시간으로 자원의 유출을 방지할 수 있는 효과가 있게 된다.

(57) 청구의 범위

청구항 1.

외부망으로부터 내부망으로의 접근요구에 대한 차단기능을 선별적으로 수행하는 방화벽과;

내부망으로부터 외부망으로의 접근요구에 대한 인증여부를 판단하고, 인증된 사용자가 외부망으로 전송하는 데이터의 복사본 및 상기 데이터 전송에 관련된 로그정보를 저장하는 FTP 프락시와;

상기 FTP 프락시의 인증을 받아 외부망의 FTP 서버와 데이터를 교환하는 복수개의 클라이언트와;

인터넷상에서 내부망의 클라이언트의 접속요구를 수용하여 각종 데이터의 교환을 수행하는 복수개의 FTP 서버와;

상기 FTP 프락시의 전송데이터 복사본을 데이터형별로 구분하여 저장하는 파일시스템과;

상기 FTP 프락시의 전송데이터에 관한 로그정보를 저장하는 데이터베이스로 구성되는 것을 특징으로 하는 네트워크망에서 내부자원의 보호기능이 강화된 보안장치.

청구항 2.

제 1항에 있어서,

상기 FTP 프락시의 로그정보를 수신하여 시스템 관리자가 인지할 수 있도록 출력하는 프락시 모니터를 더 포함하여 구성되는 것을 특징으로 하는 네트워크망에서 내부자원의 보호기능이 강화된 보안장치.

청구항 3.

내부사용자의 외부 서버에 대한 접근권한의 인증을 수행하고, 상기에서 접근권한이 인증된 사용자가 외부 서버에 접속하는 제1 단계와;

상기 제1 단계 수행 후 사용자의 명령어를 수신하여 상기 명령어가 데이터형 지정을 요구하는 것이면 지정된 데이터형을 저장하는 제2 단계와;

상기 제2 단계에서 수신한 명령어가 데이터 송신을 요구하는 것이면 데이터전송권한이 인증된 사용자의 데이터를 외부망으로 전송하고 상기 전송되는 데이터의 복사본 및 로그정보를 저장하고 시스템 관리자에게 상기 로그정보를 전송하는 제3 단계와;

상기 제2 단계에서 수신한 명령어가 데이터형 지정요구 또는 데이터 송신명령이 아닐 경우에는 해당 명령어에 따른 동작을 수행하고, 접속종료 명령어가 있게 되면 서버와의 접속을 종료하는 제4 단계를 수행하는 것을 특징으로 하는 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 운용방법.

청구항 4.

제 3항에 있어서, 사용자 인증동작은,

내부사용자의 외부서버에 대한 접속요구시 사용된 계정과 상기 계정에 할당된 패스워드 비교를 통하여 정당한 사용자인지를 판단함으로써 사용자의 인증을 수행하는 것을 특징으로 하는 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 운용방법.

청구항 5.

제 3항에 있어서, 상기 제3 단계에서 외부로 전송되는 파일의 복사본 및 로그정보의 저장동작은,

내부망에서 외부망으로 전송되는 파일을 수신하여 상기 파일의 데이터형에 따라 복사본을 파일시스템에 저장하고 외부망으로 해당 데이터를 전송하는 것을 전송완료시까지 반복적으로 수행하는 단계와;

상기 단계에서 외부망으로의 데이터 전송이 완료되면, 상기 전송과정에 대한 정보를 로그정보로써 데이터베이스에 저장하고 상기 로그정보를 시스템의 관리자가 인지할 수 있도록 출력하는 단계를 수행하는 것을 특징으로 하는 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 운용방법.

청구항 6.

제 3항에 있어서, 전송데이터에 대한 로그정보는,

상기 데이터를 전송하는 클라이언트 사용자의 계정과; 상기 클라이언트의 IP 주소와; 상기 클라이언트가 전송하는 데이터를 수신하는 FTP 서버의 IP 주소와; 상기 데이터 전송시의 날짜 및 시간과; FTP 서버로 전송된 데이터가 저장되는 절대경로 및 저장파일명과; 전송되는 데이터의 복사본 파일명 및 그 로깅경로를 포함하여 구성되는 것을 특징으로 하는 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 운용방법.

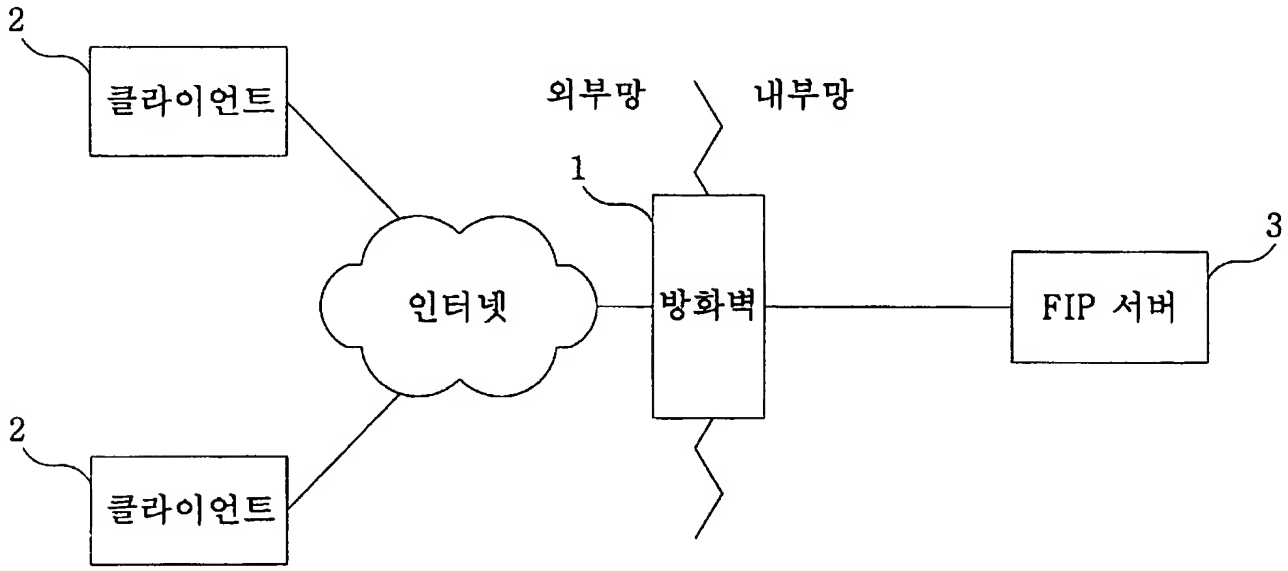
청구항 7.

제 4항에 있어서,

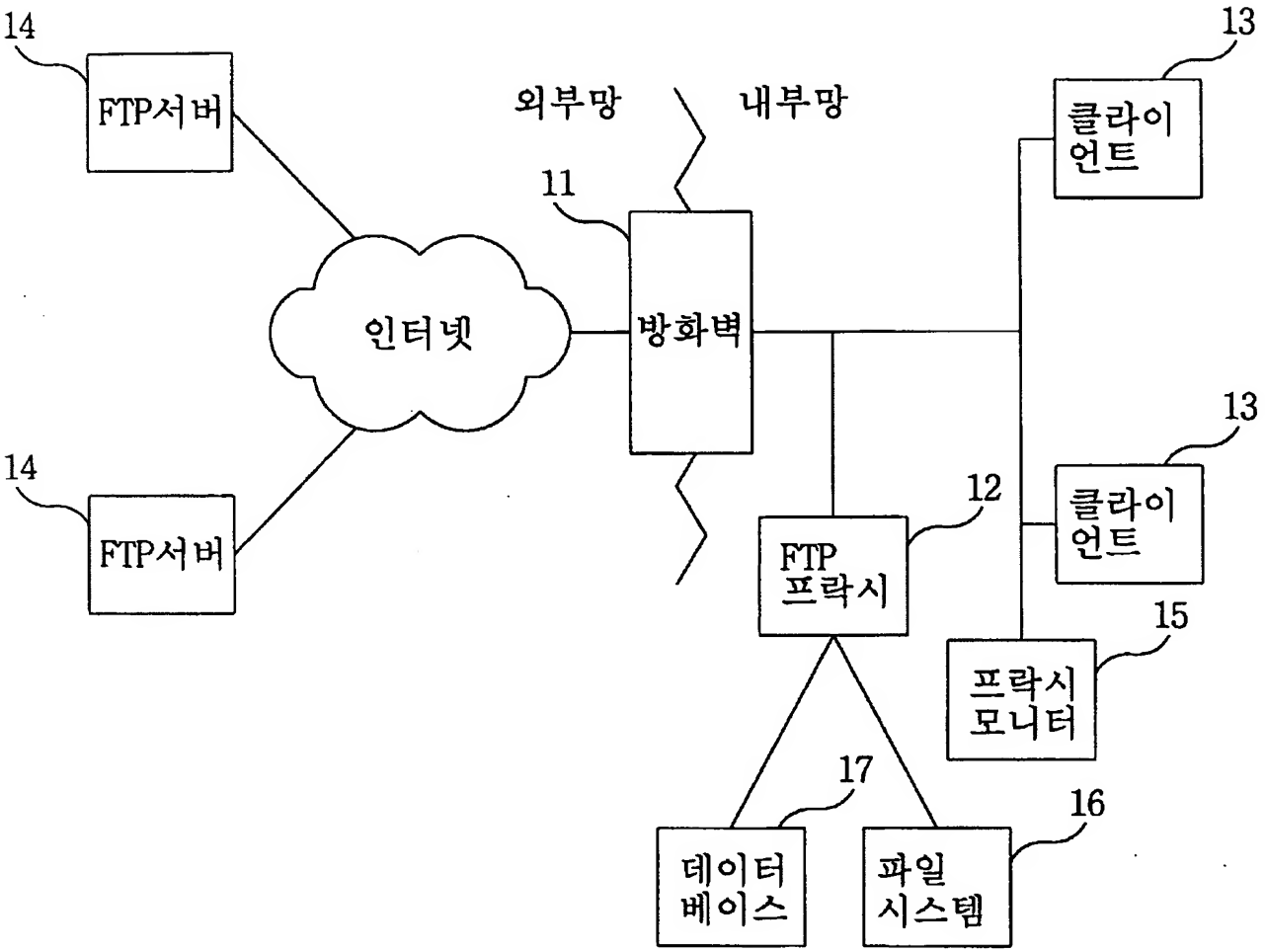
상기 사용자 인증동작은, 사용자 계정의 등록시 상기 계정이 사용될 수 있도록 특정된 호스트를 통하여 외부망에의 접속서비스를 요청하는지를 판단함으로써 내부망의 허가되지 않은 호스트를 통한 외부망에의 접속을 방지할 수 있는 접근제어를 더 포함하여 수행하는 것을 특징으로 네트워크망에서 내부자원의 보호기능이 강화된 보안장치의 운용방법.

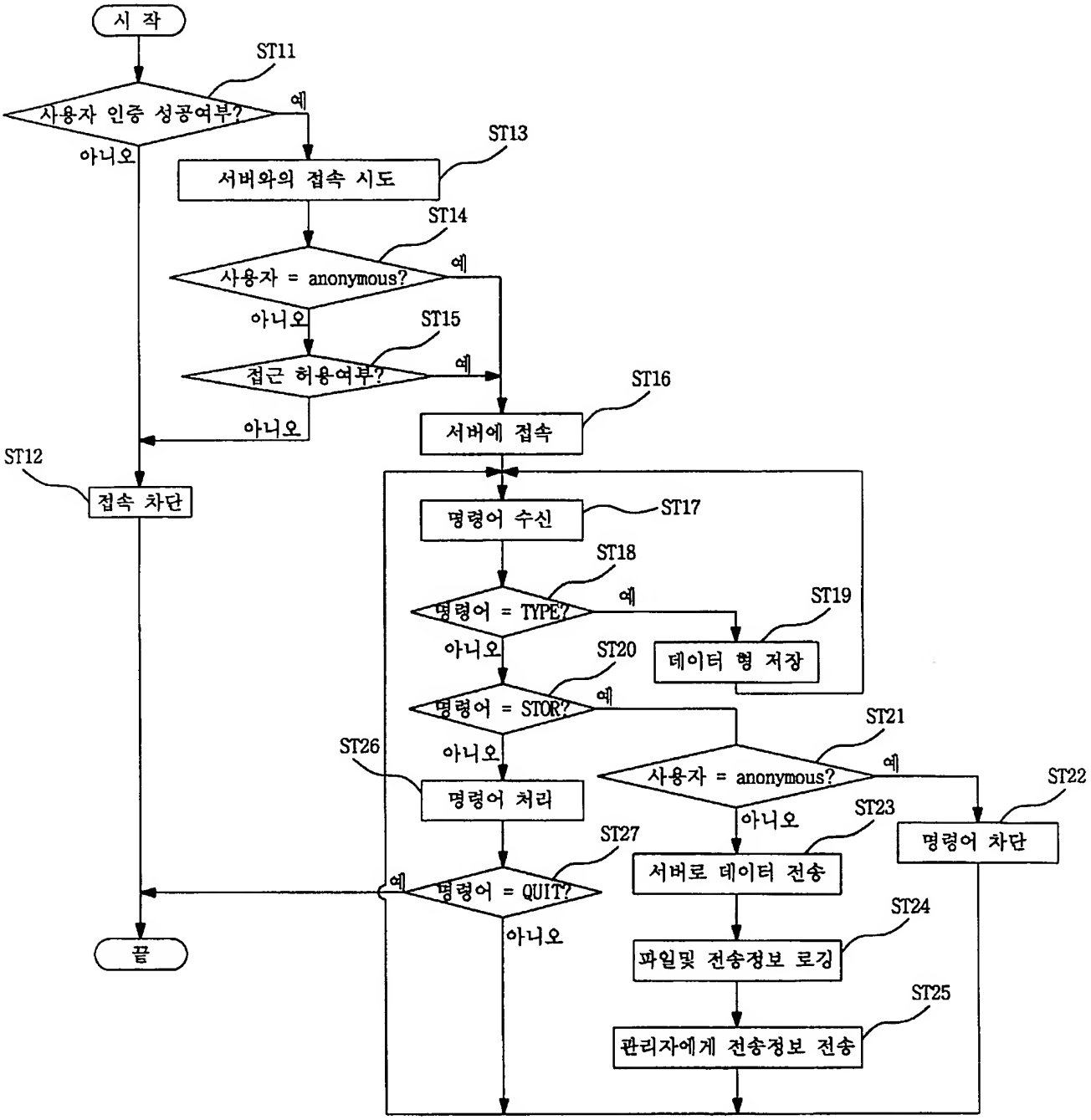
도면

도면 1

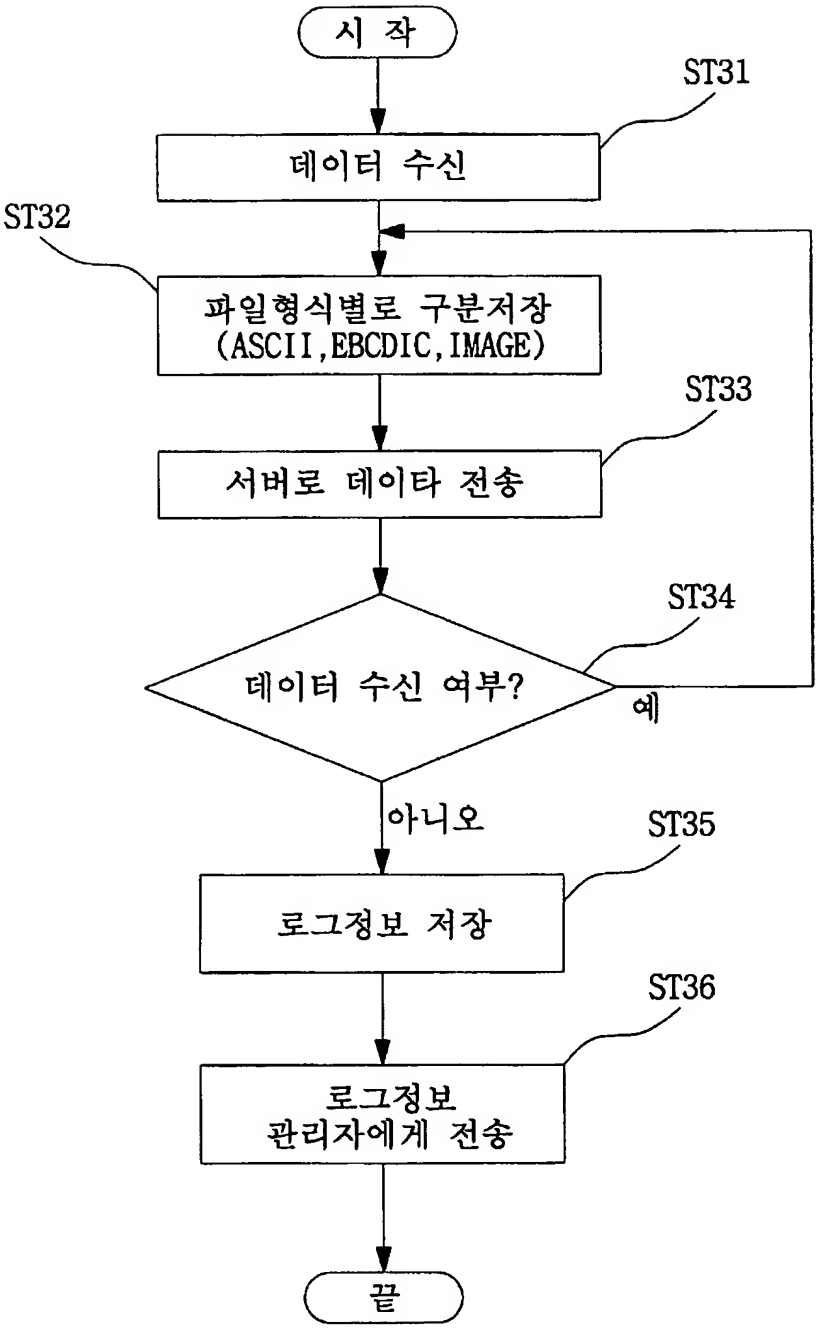


도면 2


14
FTP서버
외부망
내부망
13
클라이언트
11
인터넷
방화벽
14
FTP서버
13
클라이언트
12
FTP 프락시
15
프락시 모니터
17
16
데이터베이스
파일시스템


시 작
ST11
사용자 인증 성공여부?
예
아니오
ST13
서버와의 접속 시도
ST14
사용자 = anonymous?
예
아니오
ST15
접근 허용여부?
예
아니오
ST16
서버에 접속
ST12
접속 차단
명령어 수신
ST17
ST18
명령어 = TYPE?
예
ST19
데이터 형 저장
아니오
ST20
명령어 = STOR?
예
ST21
사용자 = anonymous?
예
ST22
명령어 차단
아니오
ST23
서버로 데이터 전송
ST26
명령어 처리
ST27
명령어 = QUIT?
예
아니오
ST24
파일및 전송정보 로깅
ST25
관리자에게 전송정보 전송
끝

도면 4



도면 5

사용자 계정	출발지 IP Address	목적지 IP Address	날짜 및 시간	전송파일명 및 저장 경로명	로깅경로 및 복사본 파일명